(xviii) $ao\,boa = aob \Rightarrow$ to (*i*)

(xix) $ao\,boa = boa \Rightarrow a = e$ thereby reducing to (*i*)

Conclusively a group with upto 5 elements is essentially abelian but for it to be non-abelian there should be at least six elements.

Problem 11. *Show that non-empty semi-group* (G, o) *forms a group if the equations* $ax = b$ *and* $ya = b$ *have unique solutions in* G $\forall$ *pair of elements* $a, b \in G$.

Since $ya = b$ is solvable for any $b \in G$, therefore by taking $b = a$, we find that $ya = a$ has a solution in G. Call this solution as e_1 so that $e_1\,a = a$ where a is a fixed element of G.

Let $c \in G$, then $ax = c$ has a solution in G.

Thus $e_1c = e_1\,(ax) = (e_1a)x = ax = c$ which follows that $e_1\; c = c \;\forall\; c \in G$, *i.e.*, e_1 is the left identity in G.

As e_1 exists in G, so $ya = e_1$ has a solution in G. Call this solution as a^{-1}. This follows that every element in G has a left inverse relative to the left identity. Hence by the theorem on §4.4, it follows that (G, o) is a group.

Problem 12. *Show that a finite-non-empty semi-group* (G, o) *forms a group if* $ab = ac \Rightarrow b = c$ *and* $ba = ca \Rightarrow b = c \;\forall\; a, b, c \in G$.

Consider a set $G = \{a_1, a_2,...a_r,...,a_p\}$ consisting of p distinct elements. Take an element a_m and multiply it to all the elements of this group,

$$a_ma_1,\ a_ma_2,....a_ma_r,......,a_ma_p.$$

All these elements will be distinct save possibly arranged in different order. If possible let us assume that

$$a_ma_r = a_ma_p \Rightarrow a_r = a_p$$

which contradicts the hypothesis that a_r and a_p are distinct elements of G. Thus

$G = \{a_ma_1,\ a_ma_2,....,\ a_ma_r,\ ....\ a_ma_p\}$ consists of p distinct elements and a_ma_l will be some element say a_r of G, *i.e.*,

$$a_ma_1 = a_r \Rightarrow ax = b \text{ has a unique solution in } G$$

Similarly we can show that

$G = \{a_1\,a_m,\ a_2a_m,....,a_ra_m,....,a_pa_m\} \Rightarrow ya = b$ has a unique solution in G.

Hence by Problem 11, the semi-group (G, o) under given conditions forms a group.

Problem 13. *Show that the set of subsets of a set with the union composition is a semi-group.*

If $S_1 = \{A, B, C,...\}$ be the set of subsets of a set S, then

S_{G1} is satisfied since, $A, B \in S$, and $A \subset S, B \subset S \Rightarrow A \cup B \subset S$ and $A, B \in S_1$, $\Rightarrow A \cup B \in S_1$, *i.e.*, the closure law is satisfied.

S_{G2} is satisfied since if $A, B, C \in S$, then associative property of union yields, $(A \cup B) \cup C = A \cup (B \cup C)$

Hence S_1 is a semi-group (by def. in §4.4).

Problem 14. *Show that the identity of a subgroup of a group is the same as that of the group.*

Let (H, o) be a subgroup of the group (G, o) and let e, e' be the identities of (G, o) and (H, o) respectively. Then

$$aoe' = a \;\forall\; a \in H$$

This equality will also hold in (G, o) as $a \in H \Rightarrow a \in G$.

Now if b be the inverse of $a \in G$, then we have

$$aoe' = a \Rightarrow bo(aoe')$$ ~~x~~ e

$$\Rightarrow (boa)oe' = boa \text{ by } G_2 \text{ for } G$$

$$\Rightarrow eoe' = e \qquad boa = e$$

$$\Rightarrow e' = e.$$

Problem 15. *Show that the inverse of an element of a subgroup of a group is the same as the inverse of the same element regarded as an element of the group.*

Let (H, o) be a subgroup of the group (G, o) and let b_1 and b_2 be the inverses of an element a as member of H and G respectively. Also let e and e' be the identities of G and H respectively. Then by Problem 14, $e = e'$,

Now $\quad aob_1 = e' = e \Rightarrow b_2o(aob_1) = b_2oe$

$$\Rightarrow (b_2oa)\, ob_1 = b_2 \text{ by } G_2, G_3 \text{ for } G.$$

$$\Rightarrow eob_1 = b_2 \qquad \because b_2oa = e$$

$$\Rightarrow b_1 = b_2.$$

Problem 16. *Show that the necessary and sufficient conditions for a complex H to be a subgroup (H, o) of a group (G, o) are*

(*i*) $a, b \in H \Rightarrow aob \in H \;\forall\; a, b$; *and* (*ii*) $a \in H \Rightarrow a^{-1} \in H \;\forall\; a$

(*Rohilkhand, 1976*)

The *conditions are necessary*, since (H, o) being a subgroup of (G, o) the composition in H (being also the composition in G) satisfies the closure law

i.e $\qquad a, b \in H \Rightarrow aob \in H \;\forall\; a, b$

which proves the first condition.

Also by Problem 14, the identity of H being the same as that of G and by Problem 15, the inverse of any element of H being the same as its inverse in G, we have

$$a \in H \Rightarrow a^{-1} \in H \;\forall\; a$$

which proves the second condition.

The *conditions are also sufficient*, since if the conditions (*i*) and (*ii*) hold then

G_1 is satisfied, for $\qquad a, b \in H \Rightarrow aob \in H$ by condition (*i*)

G_2 is satisfied, for $\qquad a, b \in H \Rightarrow aob \in H$ by (*i*) leads to

$$aob, c \in H \text{ and } a, boc \in H \;\forall\; a, b, c \in H$$

$\Rightarrow$ the same element $aoboc \in H$, *i.e.*, associative law is satisfied.

G_3 is satisfied since $\quad a \in H \Rightarrow a^{-1} \in H$ by (*ii*) leads to

$$a \in H \quad \text{and} \quad a^{-1} \in H \Rightarrow aoa^{-1} \in H \text{ by } (i)$$

But $aoa^{-1} = e$, (identity of G)

$\therefore$ $e \in H$ is an identity in H, which is also identity in G, thereby showing the existence of an identity element in H.

G_4 is satisfied since from G_3 and condition (*ii*), every element of H has an inverse.

Hence (H, o) which is a sub-group of the group (G, o) satisfies all the four exioms of group.

Problem 17. *Show that a necessary and sufficient condition for a complex H to be a subgroup (H, o) of a group (G, o) is that* $a \in H, b \in H \Rightarrow aob^{-1} \in H.$

The *condition is necessary*, since when (H, o) is a subgroup of (G, o) then by condition (*ii*) of Problem 16, we have $b \in H \Rightarrow b^{-1} \in H.$

Also by condition (*i*) of the Problem 16, $a, b^{-1} \in H \Rightarrow aob^{-1} \in H.$

Combining these two conditions we have $a \in H, b \in H \Rightarrow aob^{-1} \in H.$

The *condition is sufficient*, since if $a, b \in H \Rightarrow aob^{-1} \in H$, then we can show as below that (H, o) is a subgroup of (G, o).

The given condition yields,

$$a \in H, e \in H \Rightarrow aoa^{-1} = e \in H, e \text{ being identity of } G.$$

This follows that G_3 is satisfied, *i.e.*, $\exists$ an identity $e \in H$.

Also $e \in H, a \in H \Rightarrow eoa^{-1} = a^{-1} \in H$

i.e., G_4 is satisfied or in other words every element in H is invertible.

As such any $b \in H \Rightarrow b^{-1} \in H$

So that $a \in H, b^{-1} \in H \Rightarrow ao\,(b^{-1})^{-1} = aob \in H$

which follows that H satisfies closure law under 'o', *i.e.*, G_1 is satisfied.

Now associativity of G w.r.t. 'o' immediately follows the associativity of H w.r.t. 'o', *i.e.*, G_2 is satisfied.

Hence (H, o) is a group.

But (H, o) is a subset of (G, o).

Therefore (H, o) is a sub-group of (G, o).

Problem 18. *Show that the intersection of two subgroups of a group (G, o) is a subgroup of (G, o)*

Let (H_1, o) and (H_2, o) be the subgroups of (G, o), then

$$H_1 \cap H_2 \subset G.$$

Now $a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1, a, b \in H_2$

$\Rightarrow aob \in H_1, aob \in H_2$ since H_1, H_2 being subgroups, satisfy group axioms.

$\Rightarrow aob \in H_1 \cap H_2 \;\forall\, a, b \in H_1 \cap H_2$

Also $a \in H_1 \cap H_2 \Rightarrow a \in H_1$ and $a \in H_2$

$\Rightarrow a^{-1} \in H_1$ and $a^{-1} \in H_2$ since H_1, H_2 being subgroups satisfy group axioms.

$\Rightarrow a^{-1} \in H_1 \cap H_2.$

Hence by Problem 16, $H_1 \cap H_2$ is a subgroup of G.

Problem 19. *Show that the union of two subgroups of a group (G, o) may not be subgroup of G.*

Let (H_1, o) and (H_2, o) be the two subgroups of (G, o) and let

$a \in H_1, b \in H_2$, so that $a, b \in H_1 \overset{\cup}{\cap} H_2$. ✓ ~~$H_1 \cap H$~~ ✓

Now $a, b \in H_1 \cup H_2 \Rightarrow a \in H_1, b \in H_2 \not\Rightarrow aob \in H_1 \cup H_2$ for b may not belong to H_1.

Hence the union of two subgroups of a group may not be subgroup of the group.

Problem 20. *Show that the set $S = \{1, i, -1, -i\}$ is a subgroup of a multiplicative group of non-zero complex numbers.*

Let $(G, \cdot)$ be a multiplicative group of non-zero complex numbers. Then $(S, \cdot)$ will be a sub-group of $(G, \cdot)$ if it satisfies both the conditions for a subgroup.

The condition (i) is satisfied since $1 \cdot i = i \in S$, $1 \cdot (-1) = -1 \in S$, $1 \cdot (-i) = -i \in S$, $i \cdot (-1) = -i \in S$, $i\,(-i) = 1 \in S$, $(-1) \cdot (-i) = i \in S$.

The condition (ii) is satisfied since the inverse of 1 is $1 \in S$, the inverse of i is $-i \in S$, the inverse of -1 is $-1 \in S$ and the inverse of $-i$ is $i \in S$.

Hence $(S, \cdot)$ is a subgroup of $(G, \cdot)$.

Example 17.5 *Check the following multiplication table for the set of fourth roots* *nity, namely* $\{1, -1, i, -i\}$ *for its group properties.*

×	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
$-i$	$-i$	i	1	−1

(Burdwan and Calcutta Hons.)

Solution. The table shows that

(i) the *closure property* holds good,

(ii) the operation is *associative*,

(iii) the set has 1 as *identity element* in respect of the given operation, and

ch element has an *inverse*.

e the set forms a multiplicative group as all the group conditions are satisfied.

ner, the set is *commutative* with respect to multiplication. So, it forms an

an *group*.

● If the composition table with the corresponding operation possesses a symmetry across its main diagonal, the group is *commutative*.

► **Example 17.6** *Show that the following four* 2×2 *matrices constitute a multiplicative group :*

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \; C = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}, \; D = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix}$$

Solution. We note that A is a unit matrix. So, we have

$$AA = A, \;\; AB = BA = B,; \;\; AC = CA = C, \;\; AD = DA = D$$

Also, $$BC = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = D; \quad BD = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = C$$

Similarly, $CB = D$, $DB = C$. Also, $BB = CC = DD = A$ and $CD = DC = B$.

Hence, the composition table is as given under.

×	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

► **Example 17.7** *Show that the set* $S = \{1, \omega, \omega^2\}$, *where* ω *is a cube root of unit* *forms a finite abelian group under the composition of multiplication.* **(Burdwan Hons.)**

Solution. We have the set $S = \{1, \omega, \omega^2\}$ where $\omega^3 = 1$.

The composition table under multiplication is shown as under.

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$\because\ \omega^3 = 1;\ \omega^4 = \omega^3 \cdot \omega = \omega$

All the elements in group table belong to S so that the *closure* axiom is satisfied. Multiplication of complex numbers is associative. So, the *associativity* condition is also satisfied. Plainly, the *identity* element $1 \in S$, and the third axiom is satisfied. The *inverses* of $1, \omega, \omega^2$ are respectively $1, \omega^2, \omega \in S$ and the fourth axiom is satisfied.

The *commutative* property is also satisfied as $1 \cdot \omega = \omega \cdot 1 = \omega$ etc.

Further, the set has a *finite* number of elements and thus forms a ***finite abelian group*** under multiplication.

► **Example 17.8** *Show that the set of all nth roots of unity form a finite abelian group G of order n under multiplication.* **(Burdwan Hons.)**

Solution. The nth roots of unity by De Moivre's theorem are

$$(1)^{1/n} = (\cos 2r\pi + i \sin 2r\pi)^{1/n} = \cos 2r\pi/n + i \sin 2r\pi/n, \quad r = 0, 1, 2, \cdots, n-1$$

Thus the nth roots of unity are

$$1,\ \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},\ \cos 2\frac{2\pi}{n} + i \sin 2\frac{2\pi}{n}, \cdots, \cos\frac{(n-1)2\pi}{n} + i\sin\frac{(n-1)2\pi}{n}$$

or, $1,\ e^{1\cdot 2\pi i/n},\ e^{2\cdot 2\pi i/n}, \cdots, e^{(n-1)2\pi i/n}$.

Now, the multiplication of complex number is *associative.*

There is an *identity element,* $e^{2\pi i \cdot 0/n} = 1$.

Since $e^{2\pi i r/n} . e^{2\pi i(n-r)/n} = e^{2\pi i n/n} = e^{2\pi i} = 1$, the *inverse* of $e^{2\pi i r/n}$ is $e^{2\pi i(n-r)/n}$.

We shall now show that the product of any two elements in the set is the element of the set. If $a = e^{p\cdot 2\pi i/n}$, $b = e^{q \cdot 2\pi i/n} \in G$ where $0 \le p \le n-1$, $0 \le q \le n-1$, then $ab = e^{(p+q)2\pi i/n}$ will belong to G if $p+q \le n-1$. Assume $p+q > n-1 \Rightarrow p+q = n+m$ where $m \le n-2$, since the maximum value of $p+q$ can be $2(n-1)$, that is, $2n-2$.

$$\therefore\ ab = e^{(n+m)2\pi i/n} = e^{2\pi i} . e^{2\pi i m/n} = e^{2\pi i m/n},$$

since $e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1$.

So, all the conditions of G for being a group are satisfied.

Further, since the multiplication of complex numbers is *commutative* and the number of elements n is *finite*, G is a ***finite abelian group.***

► **Example 17.9** *Show that the set $\{1, -1, i, -i\}$ forms a cyclic group for multiplication. Find its generator.* (Calcutta Hons.)

Solution. The set $\{1, -1, i, -i\}$ forms a group under ordinary multiplication (Ex. 5).

Again, $(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = (i)^2 i = -i$, $(i)^4 = (i)^3 i = -ii = -i^2 = 1$.

Thus, the given set forms a ***cyclic group*** under ordinary multiplication whose generator is $\boldsymbol{i}$.

Since i is a generator, its inverse, i.e., $i^{-1} = -\boldsymbol{i}$ is ***also a generator*** which can be readily verified.

► **Example 17.10** *Show that the group of order 2 is always cyclic.*

Solution. If E be the identity and A another element, then $EA = A$, $AA = A^2$ are also elements of the group. So, $A^2 = A$ or E. But $A^2 \neq A$ as A is not an identity element. Hence, $A^2 = E$.

So, the group $\{A, A^2 = E\}$ is ***cyclic.***

► **Example 17.11** *Find all the generators of the cyclic group*

$$\{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$$

Solution. Let $G = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$

Since G contains all powers of a, a is a ***generator.***

Again,
$$\begin{aligned}
(a^3)^1 &= a^3,\ (a^3)^2 = a^6,\ (a^3)^3 = a^9 = a^8a^1 = ea = a,\\
(a^3)^4 &= a^{12} = a^8a^4 = ea^4 = a^4,\ (a^3)^5 = a^{15} = a^8a^7 = ea^7 = a^7\\
(a^3)^6 &= a^{18} = (a^8)^2a^2 = e^2a^2 = ea^2 = a^2\\
(a^3)^7 &= a^{21} = (a^8)^2a^5 = e^2a^5 = a^5\\
(a^3)^8 &= a^{24} = (a^8)^3 = e^3 = e
\end{aligned}$$

Since the powers of a^3 are the elements of G, a^3 is also a ***generator*** of G. Similarly, a^5 and a^7 are also the ***generators*** of G.

► **Example 17.12** *Show that the group formed by the set $\{1, \omega, \omega^2\}$, ω being the cube root of unity is a cyclic group of order 3 with respect to multiplication.*

Solution. Here $\omega^3 = 1$ is the identity and ω is the generator as its powers generate the elements $1, \omega$ and ω^2 as tabulated below.

×	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	$\omega^2 = 1$	$\omega^4 = \omega$

The group conditions are satisfied since

(i) $1\cdot\omega,\ 1\cdot\omega^2,\ \omega\cdot\omega^2 \in G$ as $\omega^3 = 1$ *(closure)*

(ii) $(1\cdot\omega)\cdot\omega^2 = 1\cdot(\omega\cdot\omega^2) = \omega\cdot\omega^2 = \omega^3 = 1$ *(associativity)*

(iii) $\omega\cdot 1 = \omega$, 1 is the identity element, *(identity)*

(iv) inverses of $1, \omega, \omega^2$ are $1, \omega^2, \omega$ respectively as $1\cdot 1 = \omega\cdot\omega^2 = \omega^2\cdot\omega = 1$ *(inverse)*

The group formed by the set $\{1, \omega, \omega^2\}$ is thus a ***cyclic group of order* 3** with generator ω.

► **Example 17.13** *If 'a' be an element of a group with identity element e and if $a^2 = a$, then show that $a = e$.* **(Calcutta Univ.)**

Solution. We have : $a^2 = a$, i.e., $aa = a \Rightarrow (aa)a^{-1} = aa^{-1} = e$.

$$\therefore\ a(aa^{-1}) = e \Rightarrow ae = e \Rightarrow \boldsymbol{a = e}. \ \textit{Hence.}$$

► **Example 17.14** *If in a group G, $x^2 = e$, identity for all x in G, i.e., every element of G (except the identity element) be of order two, prove that G is abelian.* **(Calcutta Hons.)**

Solution. Given, $x^2 = e \Rightarrow x = x^{-1}$ for all $x \in G$.

$$\therefore\ xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

$\therefore$ G is ***abelian.***

► **Example 17.15** *Prove which of the following permutations is odd or even:*

$$\text{(i)}\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \text{(ii)}\ \begin{pmatrix} 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 3 \end{pmatrix}$$

Solution. (i) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2)(1\ 3)$.

Since the permutation can be expressed as the product of *even* number of transpositions, it is an ***even*** permutation.

(ii) $\begin{pmatrix} 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 3 \end{pmatrix} = (3\ 4\ 5\ 6) = (3\ 4)(3\ 5)(3\ 6)$. Since the number of transpositions is odd, this is an *odd* permutation.

► **Example 17.16** *Prove that the set of matrices*

$$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

forms a group, an abelian group, under multiplication, α being real.

Problem 21. *Show that the order of every element of a group (G, o) of finite order is finite.*

If a be an element of (G, o) of finite order, then the positive integral powers of a, *viz.*, a, a^2, a^3, a^4 ... will all be the members of G.

But the order of G is finite, therefore all these elements of G cannot be different.

Suppose that $a^r = a^s, r > s$.

Then, $a^{r-s} = a^r o a^{-s} = a^r o a^{-r} = a^{r-r} = a^o = e$, e being the identity in G.

If $r - s = m$, then $a^{r-s} = e \Rightarrow a^m = e$, m being a positive integer as $r > s$.

This follows that $\exists$ a positive integer m s.t. $a^m = e$.

As every set of positive integers essentially possesses a least member so the set of all those positive integers s.t. $a^m = e$ has a least member known as the order of a. But a is arbitrary and hence the order of every element of G is finite.

Problem 22. *Show that the order of any power of any element a of a group is utmost equal to the order of the element.*

Assuming that order $a = m$ and order of $(a^p) = n, p \in \mathbf{I}$ (set of integers), we have order of

$$\begin{aligned} a = m &\Rightarrow a^m = e, \text{ } e \text{ being identity element.} \\ &\Rightarrow (a^m)^p = e^p \\ &\Rightarrow a^{mp} = e \\ &\Rightarrow (a^p)^m = e \\ &\Rightarrow \text{order of } (a^p) \le m \end{aligned}$$

which proves the proposition.

Problem 23. *Show that the order of any element of a group is always equal to the order of its inverse.*

Taking the orders of a and a^{-1} as m and n respectively, we have

$$a^m = e \text{ and } (a^{-1})^n = e$$

Now a^{-1} being an exponent power of a, the Problem 22 leads to order of $(a^{-1}) \le$ order of a, *i.e.*, $n \le m$.

Also since $a = (a^{-1})^{-1}$, *i.e.*, a is an exponent power of a^{-1}, so by Problem 22, we have order of $a \le$ order of (a^{-1}), *i.e.*, $m \le n$.

Hence $m \le n$ and $n \le m \Rightarrow m = n$.

Problem 24. *If a, b be two elements of a group (G, o) and $ba = a^m b^n$* $\forall$ $a, b \in G$ then *prove that the elements $a^m b^{n-2}$, $a^{m-2} b^n$ and ab^{-1} have the same order.*

We have $\quad (a^{-1}b)^{-1} = b^{-1}(a^{-1})^{-1} = b^{-1}a$

Since $b^{-1}a$ is the inverse of $a^{-1}b$, therefore by Problem 23, the order of $b^{-1}a$ and $a^{-1}b$ is the same.

Now
$$\begin{aligned} a^m b^{n-2} = a^m b^n b^{-2} &= (ba)b^{-2} \qquad \because ba = a^m b^n \\ &= b(ab^{-1})b^{-1} \quad \because b^{-2} = b^{-1}b^{-1} \end{aligned}$$

But $b\ (ab^{-1})\ b^{-1}$ has the same order as that of ab^{-1} since

$$\begin{aligned} [b\ (ab^{-1})\ b^{-1}]^2 &= [b(ab^{-1})b^{-1}]\ [b(ab^{-1})\ b^{-1}] \\ &= [b(ab^{-1})](b^{-1}b)[(ab^{-1})\ b^{-1}] \\ &= b(ab^{-1})\ (e)\ (ab^{-1})b^{-1} \\ &= b(ab^{-1})^2 b^{-1} \end{aligned}$$

or in general
$$\begin{aligned} [b(ab^{-1})\ b^{-1}]^n &= b(ab^{-1})^n b^{-1} = beb^{-1} \text{ if order of } ab^{-1} \text{ be } n \\ &= bb^{-1} = e. \end{aligned}$$

These results follow that order of ab^{-1} is the same as that of $a^m b^{n-2}$.

Again $a^{m-2}b^n = a^{-2}(a^m b^n) = a^{-2}(ba) = a^{-1}(a^{-1}b)\, a$

i.e. as above, the order of $a^{-1}b$ is the same as that of $a^{m-2}b^n$.

Problem 25. *If the elements a, b and aob of a group (G, o) are each of order 2, then show that the group is abelian.*

The order of aob being 2, we have $(aob)^2 = e$, e is the identity in G.

$$\therefore \quad (aob)\ o\ (aob)\ e \Rightarrow ao\ (aob)\ o\ (aob) = aoe$$
$$\Rightarrow ao\ (aob)\ o\ (aob)\ ob = ao\ eob$$
$$\Rightarrow (aoa)\ o\ (boa)\ o\ (bob) = ao\ eob \text{ by associative law.}$$
$$\Rightarrow a^2 o\ (boa)\ ob^2 = ao\ eob$$
$$\Rightarrow eo\ (boa)\ oe = ao\ eob \text{ since the order of } a \text{ and } b \text{ is 2.}$$
$$\Rightarrow boa = aob$$

which proves that a and b commute and hence the group is abelian.

4.5 THE CENTRE OF A GROUP

If (G, o) be a group and H be the set of those elements x ∈ G, which commute with each element in G, i.e., the set

$$H = \{x : x \in G \text{ and } aox = xoa\ \forall\ a \in G\}$$

then the set H is known as the **centre** *of G.*

Theorem. *The centre of G is a subgroup of (G, o).*

If H be the centre of G, then we have by definition

$$H = \{x : x \in G \text{ and } aox = xoa\ \forall\ a \in G\}$$

$\therefore\ x_1, x_2 \in H \Rightarrow aox_1 = x_1oa$ and $aox_2 = x_2oa\ \forall\ a \in G$.

But $\quad aox_1 = x_1oa = x_1o(x_2^{-1}ox_2)oa$, since $x_2^{-1}ox_2 = e$, the identity in H and

$$x_1oeoa = x_1oa$$
$$= (x_1ox_2^{-1})\ o\ (x_2oa)$$
$$= (x_1ox_2^{-1})\ o\ (aox_2) \qquad \because\ aox_2 = x_2oa.$$

$$\therefore \quad aox_1 = (x_1ox_2^{-1})\ o\ (aox_2) \Rightarrow (aox_1)ox_2^{-1} = (x_1ox_2^{-1})\ oa$$
$$\Rightarrow ao(x_1ox_2^{-1}) = (x_1ox_2^{-1})\ oa$$
$$\Rightarrow x_1ox_2^{-1} \text{ commutes with } a \in G$$
$$\Rightarrow x_1ox_2^{-1} \in H$$

Conclusively $x_1 \in H, x_2 \in H \Rightarrow x_1\ o\ x_2^{-1} \in H$.

Which follows by the definition of a subgroup that (H, o) is a subgroup of (G, o).

4.6 COSETS OR COSETS OF A SUBGROUP

Let (G, o) be a group, (H, o) be a subgroup of (G, o) and 'a' be an element in G, i.e., a ∈ G. Then the set

$$aH = \{ah : h \in H\} \text{ (not using the binary operation)}$$

i.e., the collection,

$$aoH = \{aoh_1, aoh_2 \ldots, aoh_i, \ldots\},\ h_i \in H$$
$$= \{aox : x \in H \text{ and } a \in G\}$$

If $a \in \mathbf{I}$ then the coset of H in $\mathbf{I}$ corresponding to a is $2\mathbf{I} + a$ since the group being abelian, $\mathbf{I} + a = a + \mathbf{I}$

$$\therefore \quad 2\mathbf{I} + 0 = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$$

$$2\mathbf{I} + 1 = \{\ldots, -5, -3, -1, 1, 3, 5, 7, \ldots\}$$

$$2\mathbf{I} + 2 = \{\ldots, -4, -2, 0, 2, 4, 6, 8, \ldots\} = 2\mathbf{I}$$

$$2\mathbf{I} + 3 = \{\ldots, -3, -1, 1, 3, 5, 7, 9, \ldots\} = 2\mathbf{I} + 1$$

$$2\mathbf{I} + 4 = \{\ldots, -2, 0, 2, 4, 6, 8, 10, \ldots\} = 2\mathbf{I}$$

$$2\mathbf{I} + 5 = \{\ldots, -1, 1, 3, 5, 7, 9, 11, \ldots\} = 2\mathbf{I} + 1 \text{ and so on.}$$

Thus the distinct cosets of H in $\mathbf{I}$ are $2\mathbf{I}$ and $2\mathbf{I} + 1$.

Clearly $\quad 2\mathbf{I} \cup (2\mathbf{I} + 1) = \mathbf{I}$.

4.7 CYCLIC GROUPS

If a group H contains an element a s.t. it is capable of being generated by the single element a i.e. every element of H is of the form a^n for some integer n, then H is said to be a **cyclic group** *and a is known as the* **generator** *of H. We also denote $H = \{a\}$.*

Hence if H is a cyclic group, then $\exists\ a \in H$, $b \in H$ s.t. $a^n = b$ (in multiplicative form) or $b = na$ (in additive form) for some integer n.

Thus $\quad H = \{a^n : n \in \mathbf{I}\}$, $a \in H$, $\mathbf{I}$ being set of integers.

e.g., the unit circle $\{z : |z| = 1\}$ in the complex plane is a cyclic group.

Characteristics of a Cyclic Group

(i) Every cyclic group is abelian.

If H be a cyclic group and a is its generator, then

$$a^m, a^n \in H \ \forall \ m, n \in \mathbf{I}$$

$$\therefore \quad a^m \circ a^n = a^{m+n} = a^{n+m} = a^n \circ a^m$$

which proves the commutative property and hence every cyclic group is abelian.

(ii) The order of a cyclic group is the same as that of its generator.

Let H be a cyclic group, a its generator and e the identity element in H. Also let n be the order of a, so that $\quad a^n = e$

Evidently, $m \in \mathbf{I}$ and $m < n \Rightarrow a^m \neq e$.

In case $m > n$, then if q be the quotient and r the least positive remainder when m is divided by n,

$$m = nq + r$$

So that $\quad a^m = a^{nq+r} = a^{nq} \circ a^r = (a^n)^q \circ a^r = e^q \circ a^r = a^r$

where $r = 0, 1, 2, \ldots. (n-1)$.

By closure axiom since $a^m \in H$, therefore n distinct elements belonging to H are a^0, $a^1, a^2, a^3, \ldots. a^{n-1}$ where $a^0 = e = a^n$.

As such there are only n elements in H and hence the order of the cyclic group H is also n which is the order of its generator.

(iii) The generators of a cyclic group of order n are the generators a^p where p is prime to n and $0 < p < n$.

$$\because\ a^n = e, \quad \therefore\ (a^p)^n = (a^n)^p = e^p = e$$

which shows that order of $a^p \leq n$.

Taking $s \in \mathbf{I}$ s.t. $o < s < n$, we have ps prime to n since n is neither a factor of p nor of s.

Let $ps = nq + r$, q being quotient and r the least positive remainder when ps is divided by n and $o \leq r \leq n - 1$.

Thus $(a^p)^s = a^{ps} = a^{nq+r} = a^{nq} \, o \, a^r = (a^n)^q \, o \, a^r = e^q \, o \, a^r = e \, o \, a^r = a^r$ where $r = 0, 1, 2, \ldots, n-1$.

It is clear that $a^r \neq e$

Hence the order of a^p is n and a^p is the generator of the group.

(iv) *A subgroup H' of a cyclic group H is also cyclic.*

Let a be the generator of H. Given that H' is a subgroup of H. Therefore every element of H and so of H' will be of the form a^n, n being an integer

Let m be the least positive integer s.t. $a^m \in H'$.

If m does not divide n then $\exists$ integers q (quotient) and r (remainder) s.t.

$$n = mq + r, o \leq r < m$$

$\therefore \quad a^n = a^{mq+r} = a^{mq} \, o \, a^r$ giving $a^r = (a^{mq})^{-1} \, oa^n$.

But $a^m \in H'$. Therefore by closure law $a^{mq} \in H'$ and so $(a^{mq})^{-1} \in H'$ since H' satisfies group axioms.

Now $\quad a^n \in H'$ (by hypothesis)

$\therefore \quad$ (1) yields, $a^r \in H'$ which contradicts the assumption that m is the least positive integer s.t. $a^m \in H'$

Thus the only possibility is that $r = 0$ and then $n = mq$ so that $a^n = a^{mq} = (a^m)^q$.

Which follows that every element a^n of H' is of the form $(a^m)^q$ showing that a^m is the generator of H' and hence H' is cyclic.

Finite cyclic groups. *If H is a cyclic group generated by a s.t. all the powers of a are not different then H = {a} is a finite cyclic group.*

If n (> 0) be the order of a, then $a^n = e$

Given any integer $s \, \exists$ two integers q and r s.t. $s = nq + r, o \leq r < n$.

$\therefore \quad a^s = a^{nq+r} = a^{nq} \, o \, a^r = (a^n)^q \, o \, a^r = e^q \, o \, a^r = e \, o \, a^r = a^r$

which follows that there are at most n distinct elements $a^1, a^2, a^3, \ldots, a^{n-1}, a^n = e$

To show that no two of these n elements are equal, let us assume if possible that

$$a^x = a^y, o < y < x < n$$

$\therefore \quad a^{x-y} = a^y \, o \, a^{-y} = a^o = e$

But $o < x - y < n$ and order of a being n, $a^{x-y} \neq e$, i.e., $a^x \neq a^y$.

Thus H contains exactly n (finite) distinct elements

$a^1, a^2, \ldots, a^{n-1}, a^n$.

Hence H is a finite cyclic group of order n.

Infinite cyclic groups. *If H be a cyclic group generated by a s.t. all the powers of a are distinct, then H = {a} is an infinite cyclic grpup.*

Let a be the generator of H. Then all the powers of a being different the order of a is zero.

Let us assume, if possible, that $a^s = a^r$ where $s > r$.

Then $a^{s-r} = a^r \, o \, a^{-r} = a^0 = e$ which contradicts the assumption that the order of a is zero.

$\therefore \quad a^s \neq a^r$

i.e., H contains an infinite number of elements and hence H is an infinite cyclic group.

Theorem 1. *In an infinite cyclic group, there are exactly two distinct generators namely one generator and the other its inverse.*

Let H be an infinite cyclic group and a, one of its generator. Then since $a^n = (a^{-1})^{-n}$, therefore a^{-1} is the other generator.

Also $a \neq a^{-1}$ otherwise $a = a^{-1} \Rightarrow aa^{-1} = a^2 = e =$ a finite cyclic group of order 2 which contradicts the hypothesis that the cyclic group is infinite.

To show that $\nexists$ third generator, if possible suppose that b is the third generator of H, so that a and b being both generators of H, $a = b^m$ and $b = a^l$,

$\therefore \quad a = (a^l)^m = a^{ml}$ .... (1)

But H being infinite cyclic group, $r \neq n \Rightarrow a^r \neq a^n$,

$\therefore$ the relation (1) is satisfied if $ml = 1$, m, l being both integers.

It follows that either $m = +1$ or $m = -1$

i.e., either $b = a$ or $b = a^{-1}$.

So that $\nexists$ third generator of H other than a and a^{-1}.

Theorem 2. *Every subgroup of an infinite cyclic group is infinite.*

Let H' be a subgroup of an infinite cyclic group H whose generator is a. Then by characteristic (*iv*) of groups, we have $H' = \{a^m\}$, m being least positive integer s.t. $a^m \in H'$.

Assume, if possible that H' is finite, then $(a^m)^n = e$ for some $n > o$ which follows that a is of finite order and so H is finite which contradicts the hypothesis.

Hence H' must be an infinite cyclic subgroup of H.

**

Problem 28. *Show that the group formed by the set $\{1, \omega, \omega^2\}$, ω being cube root of unity, i.e., $\omega^3 = 1$, is a cyclic group of order 3 with respect to multiplication.*

Here $\omega^3 = 1$ is the identity and ω is the generator as its powers generate the elements $1, \omega, \omega^2$ as tabulated:

$\cdot$	1	ω	ω
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	$\omega^3 = 1$	$\omega^4 = \omega$

The group axioms are satisfied, since if

$G = \{1, \omega, \omega^2\}$ w.r.t. '·' then

G_1—$1, \omega, \omega^2 \in G$, $1 \cdot \omega$, $1 \cdot \omega^2$, $\omega \cdot \omega^2 \in G$ as $\omega^3 = 1$

G_2—$(1 \cdot \omega) \cdot \omega^2 = 1 \cdot (\omega \cdot \omega^2) = \omega \cdot \omega^2 = \omega^3 = 1$,

G_3—1 is the identity element as $\omega \cdot 1 = \omega$ etc.

G_4— Inverses of $1, \omega, \omega^2$ are respectivley $1, \omega^2, \omega$ as

$1 \cdot 1 = \omega \cdot \omega^2 = \omega^2 \cdot \omega = 1$ (the identity element)

Hence $\{1, \omega, \omega^2\}$ is a cyclic group of order 3 with generator ω.

Problem 29. *Find all the generators of the cyclic group $\{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$ of order 8*

Let $H = \{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$

Since it contains all powers of a, so a is a generator.

Now $(a^3)^1 = a^3$, $(a^3)^2 = a^6$, $(a^3)^3 = a^9 = a^8 o a^1 = eoa = a$,

$(a^3)^4 = a^{12} = a^8 o a^4 = eoa^4 = a^4$, $(a^3)^5 = a^{15} = a^8 o a^7 = eoa^7 = a^7$

$(a^3)^6 = a^{18} = (a^8)^2 o a^2 = e^2 o a^2 = eoa^2 = a^2$

$(a^3)^7 = a^{21} = (a^8)^2\ o a^5 = e^2 o a^5 = a^5$

$(a^3)^8 = a^{24} = (a^8)^3 = e^3 = e$

Since powers of a^3 are the elements of H so a^3 is a generator of H. Similarly a^5 and a^7 are also the generators of H.

$$d \rightarrow a$$

$$(c, d) = \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix} \text{ where } \begin{array}{l} a \rightarrow a \\ b \rightarrow b \\ c \rightarrow d \\ d \rightarrow c \end{array} \text{ so that } ab + cd = ab + dc = ab + cd$$

$$(a\ b)\ (c\ d) = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} \text{ where } \begin{array}{l} a \rightarrow b \\ b \rightarrow a \\ c \rightarrow d \\ d \rightarrow c \end{array} \text{ so that } ab + cd = ba + dc = ab + cd$$

$$(a\ c)\ (b\ d) = \begin{pmatrix} a & c & b & d \\ c & a & d & b \end{pmatrix} \text{ where } \begin{array}{l} a \rightarrow c \\ c \rightarrow a \\ b \rightarrow d \\ d \rightarrow b \end{array} \text{ so that } ab + cd = cd + ab = ab + cd$$

$$(a\ d)\ (b\ c) = \begin{pmatrix} a & d & b & c \\ d & a & c & b \end{pmatrix} \text{ where } \begin{array}{l} a \rightarrow d \\ d \rightarrow a \\ b \rightarrow c \\ c \rightarrow b \end{array} \text{ so that } ab + cd = dc + ba = ab + cd$$

$$(a\ d\ b\ c) = \begin{pmatrix} a & d & b & c \\ d & b & c & a \end{pmatrix} \text{ where } \begin{array}{l} a \rightarrow d \\ d \rightarrow b \\ b \rightarrow c \\ c \rightarrow a \end{array} \text{ so that } ab + cd = dc + ab = ab + cd$$

$$\text{and } (a\ c\ b\ d) = \begin{pmatrix} a & c & b & d \\ c & b & d & a \end{pmatrix} \text{ where } \begin{array}{l} a \rightarrow c \\ c \rightarrow b \\ b \rightarrow d \\ d \rightarrow a \end{array} \text{ so that } ab + cd = cd + ba = ab + cd$$

Conclusively y_1 remains invariant by the 8 permutations mentioned above.

4.9 HOMOMORPHISM AND ISOMORPHISM OF GROUPS

(*Rohilkhand, 1989*)

Homomorphism of groups. *If* (G, o) *and* (G', o') *be two groups, then a mapping* $f : G \rightarrow G'$ *which retains the structure and is many one is called* **Homomorphism** of the **group** *G with the group G′ s.t.*

$$f(aob) = f(a)\ o'\ f(b),\ \forall\ a, b \in G.$$

We sometimes use to say that G is homomorphic to G' and denote it by $G \simeq G'$ if $\exists$ a mapping $f : G \rightarrow G'$ s.t. $f(aob) = f(a)\ o'\ f(b)\ \forall\ a, b \in G$.

Properties of homomorphism

(1) *The group* (G', o') *is a homomorphic image of the group* (G, o).

(2) *The relation of homomorphism is not symmetric, i.e.,*

$$G \simeq G' \not\Rightarrow G' \simeq G$$

(3) *The homomorphic image of the identity of the group* (G, o) *is the identity of the group* (G', o') *i.e. if* e, e' *be the identities in* G, G' *respectively then* $f(e) = e'$.

We have $\quad a \in G \Rightarrow f(a) \in G'$

and $\quad f(aoe) = f(a)\, o'\, f(e)\ \forall\ a \in G$ by definition of homomorphism.

$\therefore\ f(a)\, o'\, e = f(a) = f(aoe) = f(a)\, o'\, f(e)$ since $aoe = a$

and $\quad f(a)\, o'\, e' = f(a)$

So left cancellation law gives $e' = f(e)$.

(4) *The homomorphic image of the inverse of any element a of a group* (G, o) *is the inverse of the image of a, i.e.,* $f(a^{-1}) = [f(a)]^{-1}\ \forall\ a \in G$

We have $\quad a^{-1}, a \in G \Rightarrow f(a^{-1}), f(a) \in G'$

$$\therefore \quad f(a^{-1})\, o'\, f(a) = f(a^{-1}oa), \text{ by definition of homomorphism}$$
$$= f(e) = e' \text{ by property (3)}$$

But $\quad f(a^{-1})\, o'\, f(a) = e' \Rightarrow f(a^{-1}) = [f(a)]^{-1} \quad \because\ f(a), f(a^{-1}) \in G'$

Isomorphism of groups. *If* (G, o) *and* (G', o') *are two groups and* $\exists$ *a one-one onto mapping* $f: G \to G'$ *s.t.* $aob \xrightarrow{\text{mapped that}} a'\, ob'$ *where* $a \to a', b \to b', \forall\ a, b \in G$ *and* $a', b' \in G'$, *then the mapping f is called as* **Isomorphism** *and we say that G is* **isomorphic** *to G' and write* $G \cong G'$.

e.g., if G is an additive group of all integers, *i.e.*,

$$G = \{\ldots., -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots.\}$$

and G' is a multiplicative group of all positive and negative powers of an integer 2 *i.e.*

$$G' = \{2^m : m = 0, \pm 1, \pm 2 \ldots.\}$$
$$= \left\{\ldots.\frac{1}{16}, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \ldots..\right\}$$

Then we have $\quad f(m) = 2^m$, m being an integer

and $\quad f(m+n) = 2^{m+n} = 2^m \cdot 2^n = f(m) \cdot f(n)$, m, n being integers.

This shows that f is one-one onto and retains the group structure and hence $G \cong G'$.

Properties of isomorphism

(i) *The order of G = the order of G'*

(ii) *For isomorphic groups* (G, o) *and* (G', o') *the identity* e' *of* G' *is the image of identity e of G, i.e.,* $f(e) = e'$.

If $a \in G$ and $a' \in G'$ then $a' = f(a)$

$\therefore\ f: G \to G'$ is one-one onto $\Rightarrow f(a) \in G'\ \forall\ a \in G.$

$\Rightarrow f(e) \in G' \quad \because\ e \in G$

Now $\quad aoe = a \Rightarrow f(aoe) = f(a)$

$\Rightarrow f(a)\, o'\, f(e) = f(a)\, o'\, e'$ by definition of isomorphism

$\Rightarrow a'\, o'\, f(e) = a'\, o'\, e'$

$\Rightarrow f(e) = e'$ by left cancellation law.

(iii) *For isomorphic groups* (G, o) *and* (G', o') *the image of inverse of any element a of G is the inverse of the image of a, i.e.*

$$f(a^{-1}) = [f(a)]^{-1}$$

If e, e' are identities of G, G' respectively then by property (*ii*) $f(e) = e'$

Also we have $a^{-1}oa = e = aoa^{-1}\ \forall\ a \in G$

But $a^{-1}oa = e \Rightarrow f(a^{-1}oa) = f(e)\ \forall\ a \in G$

$\Rightarrow f(a^{-1})o'f(a) = e'$ by definition of isomorphism

$\Rightarrow f(a^{-1}) = [f(a)]^{-1}$ by definition of inverse of an element in G'

(*iv*) *For isomorphic groups* (G, o) *and* (G', o'), *the order of an element* $a \in G$ *is the same as the order of its image* $a' \in G'$.

$f: G \to G'$ is one-one and onto.

If e, e' be identities in G, G' respectively, then

$f(e) = e'$ and $f(aob) = f(a)\ o'\ f(b)\ \forall\ a, b \in G.$

If n be the order of an element $a \in G$ then $a^n = e$

Also if m be the order of $f(a)$ then $[f(a)]^m = e'$

But $\quad a^n = e \Rightarrow f(a^n) = f(e)$

$\Rightarrow f(aoaoa...n \text{ times}) = e'$

$\Rightarrow f(a)\ o'\ f(a)\ o'\ ....n$ times $= e'$ by definition of isomorphism

$\Rightarrow [f(a)]^n = e'$

$\Rightarrow$ order of $f(a) \le n$

$\Rightarrow m \le n.$

Also $[f(a)]^m = e' \Rightarrow f(a)\ o', f(a)\ o',...m$ times $= f(e)$

$\Rightarrow f(aoaoa...m \text{ times}) = f(e)$ by definition of isomorphism

$\Rightarrow f(a^m) = f(e)$

$\Rightarrow a^m = e \quad \because f$ is one-one

$\Rightarrow$ order of $a \le m$

$\Rightarrow n \le m$

So that $m \le n$ and $n \le m \Rightarrow m = n$

$\Rightarrow$ order of a = order of a'.

(*v*) *If f is isomorphic mapping of* $G \to G'$, *then* f^{-1} *is also isomorphic.*

If f is one-one and onto then f^{-1} exists and is also one-one onto.

Also if $\quad x = f(a), y = f(b)$ for $a, b \in G$ and $x, y \in G'$, then

$a = f^{-1}(x), b = f^{-1}(y)$

But $\quad f^{-1}(xo'y) = f^{-1}[f(a)\ o'\ f(b)]$

$= f^{-1}[f(aob)] \because f$ is isomorphic mapping

$\Rightarrow aob \quad \because f^{-1}f(p) = p.$

$\Rightarrow f^{-1}(x)\ o\ f^{-1}(y)$

which follows that f^{-1} retains the group structure and hence f^{-1} is isomorphic.

Automorphism of groups. *An isomorphism of a group onto itself is said to be an* **automorphism** *of the group e.g.* $f: G \to G'$ *given by* $f(a) = a^{-1}$, $a \in G$ *is an automorphism iff G is an abelian group.*

In other words an automorphism f of G is a one-one transformation of G onto itself s.t. $(xy)f = (xf)\ (yf)\ \forall\ x, y \in G$

i.e., $\quad f(xy) = f(x) f(y)$

As another example the identity mapping $i: G \to G$ is an automorphism of group G.

Conjugate subgroups. *If x, y, z, etc. be the elements of a group G i.e. $x, y, z, \ldots \in G$, then the subgroups H, $x^{-1}Hx$, $y^{-1}Hy$, $z^{-1}Hz$,...., are known as the* **conjugate subgroups** *of G.*

Normal Subgroups (or Normal divisor or Invariant subgroup or Self-conjugate subgroup). *A subgroup H of a group G is said to be a* **normal subgroup** *of G if $\forall\, x \in G$, $x^{-1} Hx = H$ or equivalently, if $Hx = xH \;\forall\; x \in G$.*

Properties of normal subgroups

(*a*) *If e be the identity in G, then the whole group G and $\{e\}$ are normal subgroups of G*

group G is normal since a left coset its composition table is as shown here.

Evidently G/H is a cyclic group generated by $\{a, a^4\}$.

	$\{e, a^3\}$	$\{a, a^4\}$	$\{a^2, a^5\}$
$\{e, a^3\}$	$\{e, a^3\}$	$\{e, a^4\}$	$\{a^2, a^5\}$
$\{a, a^4\}$	$\{a, a^4\}$	$\{a^2, a^5\}$	$\{e, a^3\}$
$\{a^2, a^5\}$	$\{a^2, a^5\}$	$\{e, a^3\}$	$\{a, a^4\}$

Jw6

7.11 COMPLEXES AND KERNEL

Complex of a group. *A non-empty subset H of a group G is called as a* **complex** *of the group G.*

Properties of complexes

(i) *If Z be a complex containing the elements a, b, c of a group G then Z = {a, b, c}*

(ii) *If Z = {a, b, c} be a complex then aZ = $\{a^2, ab, ac\}$ etc.*

(iii) *If Z_1 and Z_2 be two complexes of a group G, then the product of Z_1, Z_2 is defined as*

$$Z_1 Z_2 = \{x : x = z_1 z_2, z_1 \in Z_1, z_2 \in Z_2\}$$

Now since $z_1 \in Z_1$, $z_2 \in Z_2$ and $Z_1, Z_2 \subset G$

$\therefore \quad z_1 z_2 = x \in G$ by closure axiom.

As such $Z_1 Z_2 \subset G$.

Which follows that $Z_1 Z_2$ is also a complex of G, obtained by multiplying every element in Z_1 with every element in Z_2.

(iv) *The subgroup H of a group G also gives a complex s.t. $HH = H^2 = H$.*

(v) *A group can be expressed as a sum of complexes.*

Image of a group G under a mapping f. *If $f : G \to G'$ be a homomorphism of a group G into a group G′, then $f(G) = \{f(x) \in G' : x \in G\}$ is a subset of G′ and is termed as the* **Image of G under** *f and denoted by Im (f).*

Kernel of f. *If $f : G \to G'$ be a homomorphism of G into G′, then the subset of those elements of G which are mapped onto the identity of G′ under f′ is said to be the* **Kernel of f** *and denoted by ker (f) or $f^{-1}(e')$.*

i.e., $\ker(f) = \{x \in G : f(x) = e'\}$

Propositions relating to Kernel

I. *A homomorphism $f : G \to G'$ is an isomorphism iff ker $f = \{e\}$.*

Assuming that $f : G \to G'$ is an isomorphism, if $a \in \ker f$ then

$$f(a) = e' = f(e),\ e' \text{ being identity in } G'.$$

Now f being one-one and $a = e$, kernel of f consists of e only. Conversely if ker $f = \{e\}$ for f to be homomorphism, and if $a, b \in G$ s.t. $f(a) = f(b)$, then

$$\begin{aligned} f(ab^{-1}) &= f(a)\,f(b^{-1}) \\ &= f(a)\,[f(b)]^{-1} \\ &= e' \qquad \because f(a) = f(b) \\ \therefore \quad ab^{-1} &\in \ker f \\ \text{or} \quad ab^{-1} &= e \\ \text{or} \quad a &= b \end{aligned}$$

So f is one-one and hence f is an isomorphism.

II. *If f be homomorphism of G′ then ker (f) is an invariant subgroup of G.*

If $a, b \in \ker(f)$, then $f(a) = e' = f(b)$, e' being identity of G.

$\therefore \quad f(ab) = f(a)\,f(b) = e'\,e' = e'$

which implies that $ab \in \ker(f)$, *i.e.*, closure axiom is satisfied.

Now ker (f) being a subset of G, associativity axiom is self-evident.

Again $f(e) = e' \Rightarrow e \in \ker(f)$, e being identity in G.

Therefore, there exists an identity in G.

Further if $a \in \ker(f)$ then $f(a^{-1}) = [f(a)]^{-1} = (e')^{-1} = e'$

which shows that $a^{-1} \in \ker(f)$ when $a \in \ker(f)$.

This follows the existence of an inverse in G.

As such ker (f) is a subgroup of G, as ker (f) satisfies all the four group axioms.

Moreover ker (f) is an invariant subgroup of G as is shown below :

If $g \in G$ and $h \in \ker(f)$, then

$$\begin{aligned} f(g^{-1}hg) &= f(g^{-1})\,f(h)\,f(g) \\ &= [f(g)]^{-1}\,e'\,f(g) \qquad \because h \in \ker(f) \Rightarrow f(h) = e' \\ &= [f(g)]^{-1}\,f(g) \\ &= e' \end{aligned}$$

$\therefore \quad g^{-1}hg \in \ker(f)$.

Hence ker (f) is an invariant subgroup of G.

Note 1. It is easy to show that Im (f) is a subgroup of G.

III. *If H be a normal subgroup of a group G, then there is a homomorphism of G onto G/H.*

Let $f : G \to G/H$ be given by $f(x) = Hx\ \forall\ x \in G$

$\because\ \forall\ x \in G, \exists$ a unique coset Hx, f is a mapping.

Also the binary operation in G/H being defined by

$$(Hx)\ (Hy) = H\ (xy)$$

We have

$$f(xy) = H\ (xy) = (Hx)\ (Hy) = f(x)\ f(y)$$

Which follows that f is a homomorphism and it is onto since every coset $Hz \in G/H$ has z as its preimage in G.

Note 2. **Natural Homomorphism.** The homorphism $f : G \to G/H$ given by $f(x) = Hx$ is known as **Natural Homomorphism** or **Canonical Homomorphism** of G onto G/H.

IV. *If f be a homomorphism of a group G onto a group G' with kernel k, then*

$$G/K \cong G'$$

Consider the mapping $\phi : G/K \to G'$ defined by $\phi\ (Kx) = f(x)$

Taking $Kx = Ky$, we have $xy^{-1} \in K$ and $f(xy^{-1}) = e'$, e' being identity in G', *i.e.*, $f(x)$ $f(y^{-1}) = e'$

or $f(x)\ [f(y)]^{-1} = e'$

or $f(x) = f(y)$.

This follows that ϕ is uniquely defined.

Now if $f(y) \in G'$ then Ky is the preimage of $f(y)$ in G/K under ϕ.

This follows that ϕ is onto.

Again f will be one-one if $Kx = Ky$ provided $f(x) = f(y)$.

Take an element $z = xy^{-1} \in G$ *i.e.* $zy = x$

$$\begin{aligned} \therefore \quad f(z) = f(xy^{-1}) &= f(x)\ f(y^{-1}) \\ &= f(x)\ [f(y)]^{-1} \\ &= e' \qquad \because f(x) = f(y) \end{aligned}$$

So that $z \in K$ and $Kx = K(zy) = (Kz)y = Ky$

$\therefore$ ϕ is one-one.

Further to show that f preserves the structure, we have

$$\phi(Kx)\ \phi(Ky) = f(x)\ f(y) = f(xy) = \phi\ [K\ (xy)] = \phi\ [(Kx)\ (Ky)]$$

Hence ϕ is isomorphism and thus $G/K \cong G'$.

V. *If f is a homomorphism from the group (G, o) into the group (G', o') then the pair $(\ker f, o)$ is a normal subgroup of (G, o).*

Evidently $\ker f \neq \phi$ (non-empty) since $e \in \ker f$ and $\ker f \subset G$

Now $a, b \in \ker f \Rightarrow f(a) = e', f(b) = e'$

But $f(b^{-1}) = [f(b)]^{-1} = [e']^{-1} = e'$

$\therefore f(aob^{-1}) = f(a)\ o\ [f(b)]^{-1} = e'oe' = e'$

$\therefore a, b \in \ker f \Rightarrow aob^{-1} \in \ker f$

Hence $(\ker f, o)$ is a subgroup.

Again $\forall\ a \in G$ and $h \in \ker f$, we have

$$\begin{aligned} f(ao\ hoa^{-1}) &= f(a)\ o\ f(h)\ o\ f(a^{-1}) \\ &= f(a)\ o\ f(h)\ o\ [f(a)]^{-1} \\ &= f(a)\ oe'\ o\ [f(a)]^{-1} \\ &= f(a)\ o\ [f(a)]^{-1} \\ &= e' \end{aligned}$$

$\therefore$ $\forall\ a \in G$ and $h \in \ker f \Rightarrow aohoa^{-1} \in \ker f$

Since [illegible] representations are [illegible] of order $m + n$ [illegible] adding these [illegible]tion in which two representations consisting of m square matrices of order m [illegible] representations such as

$$\begin{array}{cccl} \left[\begin{array}{c} \mu \\ O \\ \leftrightarrow \end{array}\right. & \begin{array}{c} \vdots \\ \vdots \\ \ \end{array} & \left.\begin{array}{c} O \\ \mu' \\ \leftrightarrow \end{array}\right] & \begin{array}{l} \updownarrow n \text{ rows} \\ \\ \updownarrow p \text{ rows} \end{array} \\ n & & p & \\ \text{columns} & & \text{columns} & \end{array} \quad \text{.... (1)}$$

whose elements are

$$\begin{bmatrix} \mu(A_1), & O \\ O, & \mu'(A_1) \end{bmatrix}, \begin{bmatrix} \mu(A_2), & O \\ O, & \mu'(A_2) \end{bmatrix}, \ldots\ldots, \begin{bmatrix} \mu(A_m), & O \\ O, & \mu'(A_m) \end{bmatrix}, \quad \text{.... (2)}$$

Calling the first representation as μ_1, second as μ_2 and their sum as μ we have

$$\mu_1 + \mu_2 = \mu \quad \text{.... (3)}$$

Reducible representation. A representation arising from the representation (2) by similarity transformation is called as *reducible* representation and clearly these transformations are equivalent to the representation of the form (2). Other representations for which this is not possible are termed *irreducible representations.*

For example, A reducible matrix can be put in the form (2), by similarity transformation by means of converting jth row and column into j'th row and column. In order to effect this reducible representation take an isomorphic linear operator $T : L \rightarrow L'$, L, L' being two linear spaces and matrices, $A, B, ... \in L, A', B' .... \in L'$

We have $\quad A' = TAT^{-1}, B' = TBT^{-1}$ .... etc.

If we choose $T_{\alpha\beta} = \delta_{\alpha\beta}$, then $(T^{-1})_{jk} = \delta'_{jk}$

and $\sum\limits_{\beta} T_{\alpha\beta}(T^{-1})_{\beta j} = \sum\limits_{\beta} \delta'_{\alpha\beta}\delta'_{\beta j} = \delta_{\alpha j}$

So that the similarity transformation for this T resumes the required renumbering such that

$$\begin{aligned} \bar{A} &= T^{-1}AT \\ &= A'_{jk} \text{ where } \left(\bar{A}\right)_{jk} = \sum_{\alpha\beta} \delta'_{j\alpha} A_{\alpha\beta} \delta'_{\beta j} \end{aligned}$$

Now we know that every non-singular matrix $\mu(A)$ is invertible and multiplication on any group element A with identity element E gives A, so the multiplication of any representation matrix $\mu(A)$, *i.e.*,

$$\mu(A)\mu(E) = \mu(A) \text{ so that } \mu(E) = I, \text{ a unit matrix}$$

As such the unit matrix may be associated with the identity element of the group and we have

$$\mu(A)\,\mu(A^{-1}) = \mu(AA^{-1}) = \mu(E) = I$$

i.e.,

$$[\mu(A)]^{-1} = \mu(A^{-1}) \quad \text{... (4)}$$